

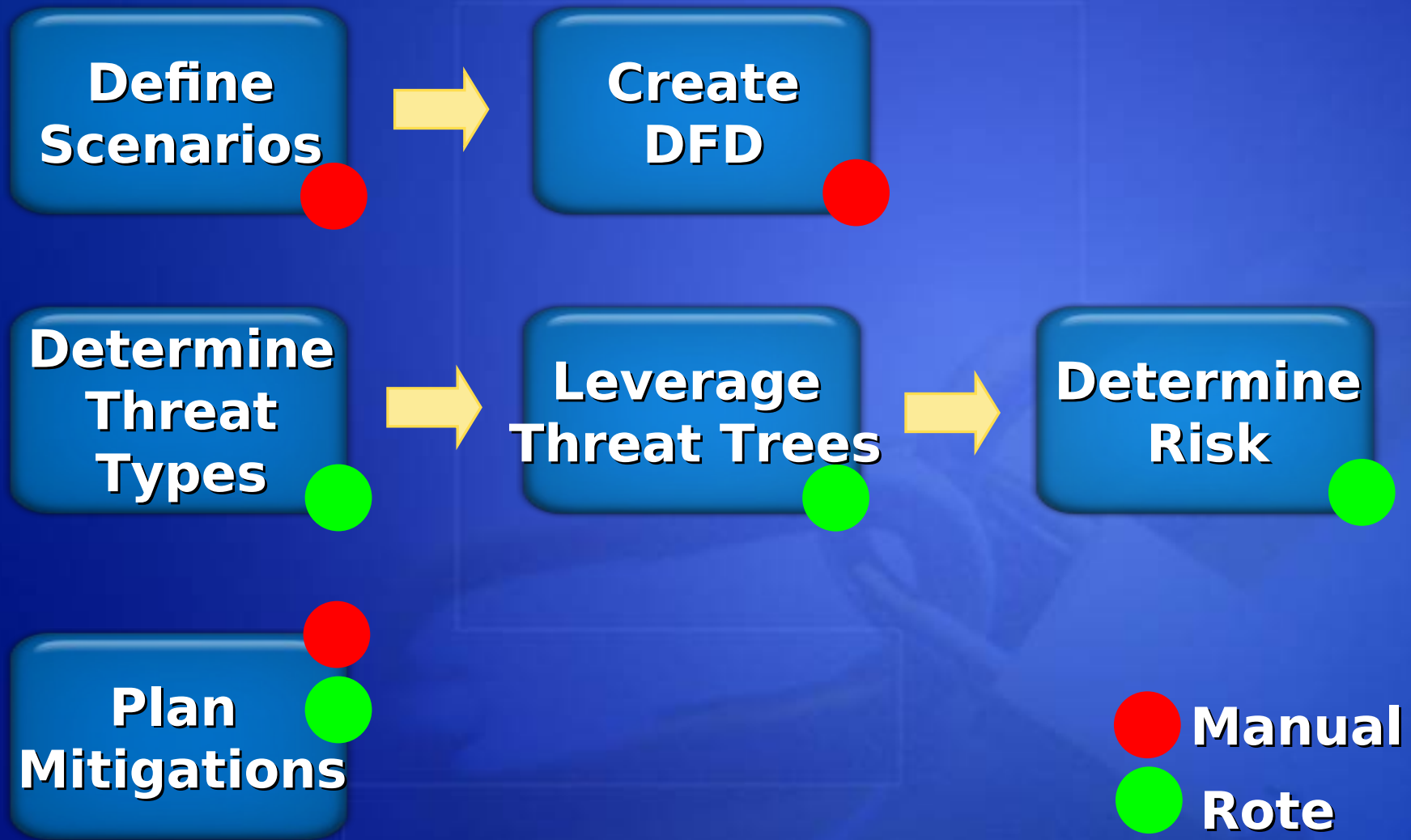
Introduction to Threat Modeling

Michael Howard, CISSP
Senior Security Program
Manager
Security Engineering and
Communication

Threat Analysis

- The goal of threat modeling is to:
 - Find security design flaws
 - Mitigate the threats
 - Reduce risk

The Updated Threat Modeling Process



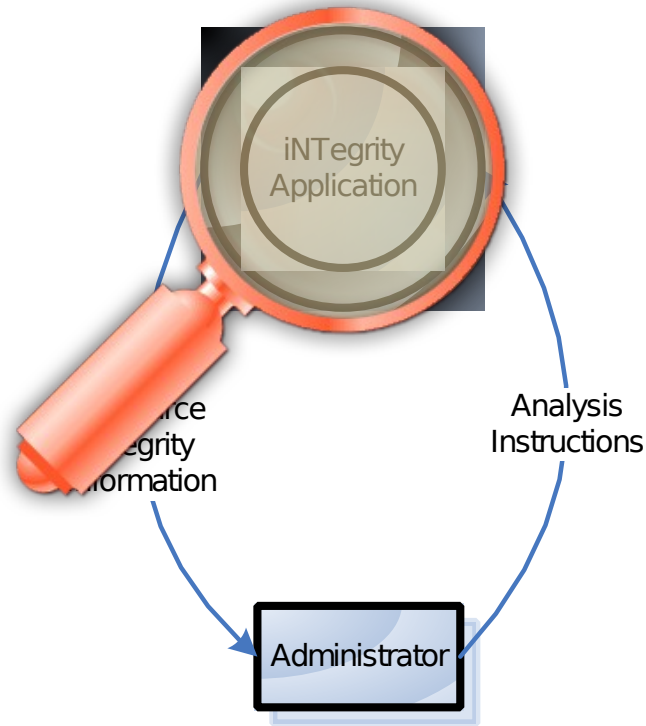
Define Scenarios & Background Info

- Define the most common and realistic use scenarios for the application
 - Example from Windows Server 2003 and Internet Explorer
 - “Admin browsing the Internet from a Domain Controller”
 - Example from Windows CE
 - “The stolen device”
- Define your users

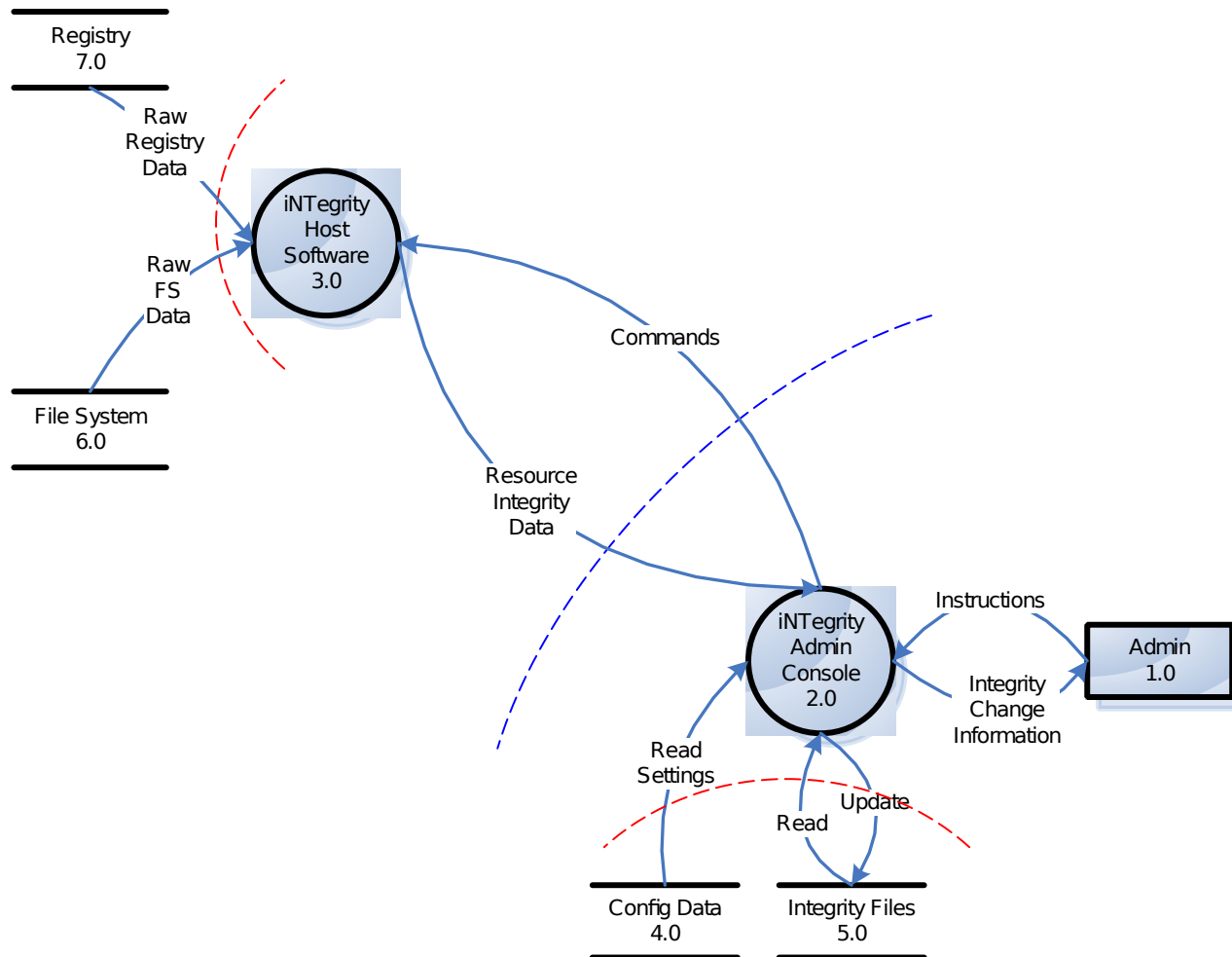
Data Flow Diagrams (DFDs)

- A DFD is a graphical representation of how data enters, leaves, and traverses your component
 - It is not a Class Diagram or Flow Chart!
 - Shows all data sources and destinations
 - Shows all relevant processes that data goes through
- Good DFDs are critical to the process
 - This point can't be emphasised enough!
 - Building DFDs == understanding the system
 - Analysing DFDs == understanding the

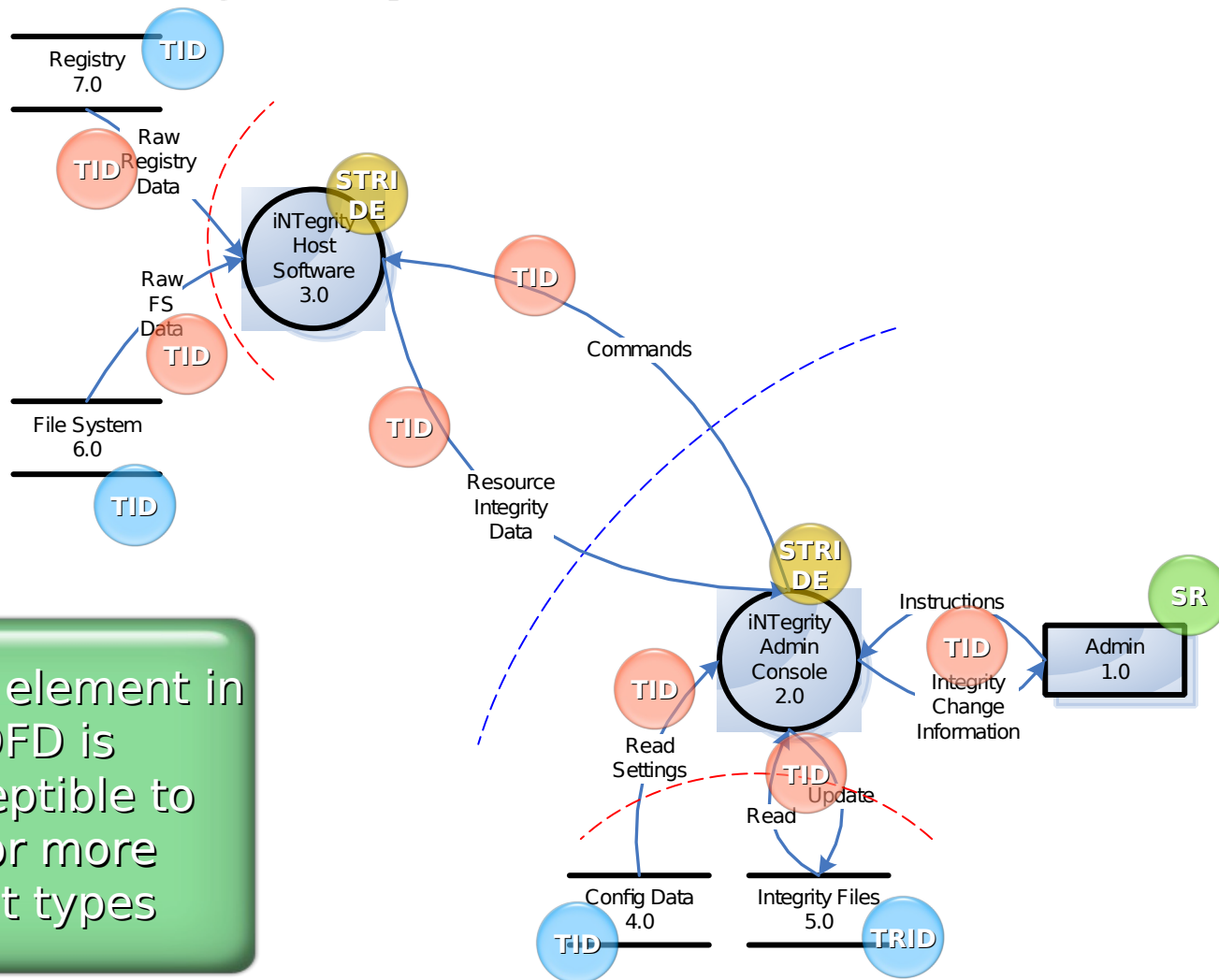
Context Diagram: An Integrity Checker



Level-0 DFD: An Integrity Checker



Level-0 DFD: An Integrity Checker



Each element in the DFD is susceptible to one or more threat types

STRIDE

A Taxonomy of Threat Types

- A more fine-grained version of CIA, but from an attacker's perspective
 - Spoofing
 - Tampering
 - Repudiation
 - Information Disclosure
 - Denial of Service
 - Elevation of Privilege

DFD Elements are Targets

A “Work list”

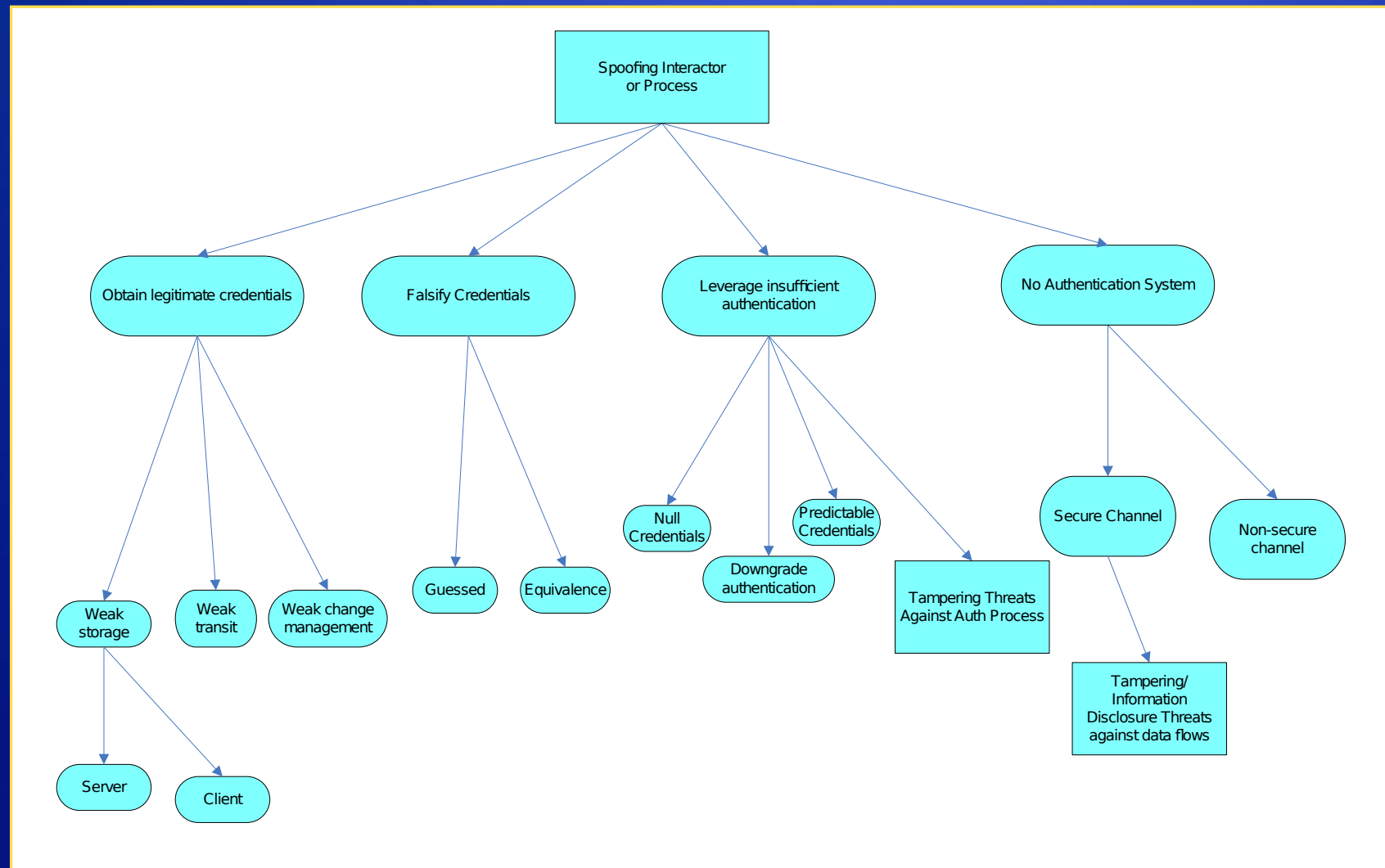
Data Flow	S	T	R	I	D	E
1→2		✓		✓	✓	
2→1		✓		✓	✓	
2→4		✓		✓	✓	
4→2		✓		✓	✓	
2→5		✓		✓	✓	
5→2		✓		✓	✓	
2→3		✓		✓	✓	
3→2		✓		✓	✓	
6→3		✓		✓	✓	
3→6		✓		✓	✓	
7→3		✓		✓	✓	
3→7		✓		✓	✓	
Data Store						
6		✓		✓	✓	
7		✓		✓	✓	
4		✓		✓	✓	
5		✓		✓	✓	
Process						
3	✓	✓	✓	✓	✓	✓
External Entity						
1	✓		✓			

Each ✓ is a potential threat to the system.

Each threat is governed by the conditions which make the threat possible

Threat Tree Pattern Examples

Spoofing



A Special Note about Information Disclosure Threats

**All information disclosure
threats are potential
privacy issues.**

Raising the Risk.

Is the data sensitive or PII?

Calculating Risk with Numbers

- DREAD etc.
- Very subjective
- Often requires the analyst be a security expert
 - On a scale of 0.0 to 1.0, just how likely is it that an attacker could access a private key?
- Where do you draw the line?
 - Do you fix everything above 0.4 risk and leave everything below as “Won’t Fix”?

Calculating Risk with Heuristics

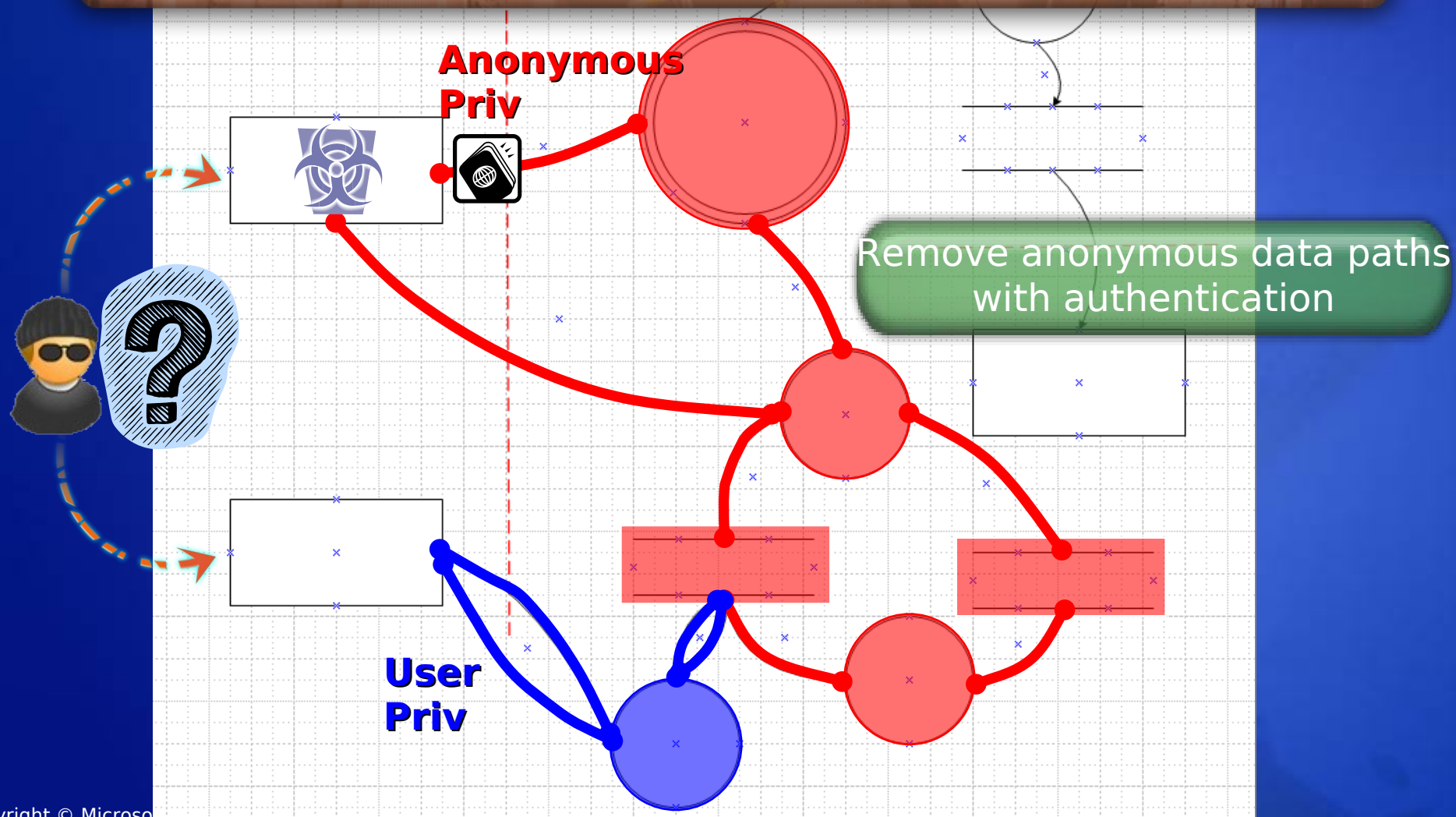
- Simple rules of thumb
- Real-world data
- Similar heuristics as the MSRC bulletin rankings

Mitigation Techniques

Threat	Mitigation Feature
Spoofing	Authentication
Tampering	Integrity
Repudiation	Nonrepudiation
Information Disclosure	Confidentiality
Denial of Service	Availability
Elevation of Privilege	Authorization

Code Review and the DFD

Review code and data on the anonymous data flows, the threat path – this is where the bad guys go – they follow the line of least-resistance.



Testing Threats

Threat Modeling GUI - C:\Program Files\Microsoft\Threat Modeling Tool\Samples\Humongous Insurance Price Quote Web Site.tmd

File Edit Tools Help

Humongous Insurance Price Quote Web Site

- Background Information
- Entry Points and Assets
- Threats
 - Adversary uses SQL special characters to access the database
 - Adversary acquires another user's login data
 - Threat Tree
 - Adversary gets user's login data
 - Adversary uses phishing to get user's login data
 - Adversary gets user to disclose user's login data
 - Adversary gets a valid password
 - Adversary has direct access to the database
 - Adversary uses a brute-force attack to guess the password
 - Adversary guesses the password
 - Adversary gets user to disclose password
 - Username validity confirmation via login page
 - User's login data
 - Insurance agent's login data
 - Login page
 - Database stored procedures
 - The database server should not allow password quality
 - There is no password quality
 - Adversary acquires another user's login data
 - Adversary retrieves another user's login data
 - Adversary accesses the backend database
 - Adversary modifies a user's price
 - Adversary accesses insurance agent's login data
 - Adversary prevents a user from logging in
 - Adversary prevents insurance agent from logging in
 - The list of quote requests is not updated
 - Notification of new quote request
 - Remote user with login credentials
 - Insurance agent
 - Insurance agent quote review
 - Insurance agent
 - HTTPS user
 - RetrieveData function
 - Insurance agent

STRIDE Classification

☒ Spoofing ☐ Tampering ☐ Repudiation ☒ Information Disclosure ☐ Denial of Service ☒ Elevation of Privilege

Entry Points: (1.1) Login page (2.1) Database stored procedures

Protected Resources: (13.1) User's login data (13.7) Insurance agent's login data

Remove New New

Adversary acquires another user's login data

Adversary retrieves another user's login data

Adversary accesses the backend database

Adversary modifies a user's price

Adversary accesses insurance agent's login data

Adversary prevents a user from logging in

Adversary prevents insurance agent from logging in

What needs testing

Microsoft Confidential

Threat Model Checklist

- ✓ No design is complete without a threat model!
- ✓ Follow anonymous data paths
- ✓ Every threat needs a security test plan
- ✓ Check all information disclosure threats - are they privacy issues?
- ✓ Be wary of elevated processes
- ✓ Use the threat modeling tool (<http://msdn.microsoft.com>)